REMARKS

Reconsideration and allowance of the present application are respectfully requested. Claims 1-18 are pending in the application. By this amendment, a substitute Abstract is provided; and claims 1-4, 6-8 and 10 are amended; and claims 11-18 are added. No new matter is added.

Specification

In numbered paragraph 1, page 2 of the Office Action, the Examiner objects to the abstract. To address the Examiner's concerns, a substitute abstract is provided. Withdrawal of the objection to the abstract of the disclosure is respectfully requested.

Claims Objection

In numbered paragraph 2, page 2 of the Office Action, the Examiner objects to claims 1-10. To address the Examiner's specific concerns, claims 1, 3 and 8 are amended. Withdrawal of the objection to claims 1-10 is respectfully requested.

35 U.S.C. § 112

In numbered paragraph 3, bridging pages 2 and 3 of the Office Action, claims 2, (3), 6, 7 and 10 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite. To address the Examiner's specific concerns, claims 2, 3, 6, 7 and 10 are amended. Withdrawal of the rejection of claims 2, 3, 6, 7 and 10 under 35 U.S.C. §112 is respectfully requested.

35 U.S.C. §§102 and 103

In numbered paragraph 5, pages 4 and 5 of the Office Action, claims 1-3, 5, 6, 8 and 9 are rejected under 35 U.S.C. §102(e) as allegedly being anticipated by US 2004/0261030 (Nazzal). In numbered paragraph 7, page 6 of the Office Action,

dependent claim 4 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the Nazzal publication, in view of Symantec Antivirus for Macintosh copyright 1994. In numbered paragraph 8, bridging pages 6 and 7 of the Office Action, dependent claim 7 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the Nazzal publication, in view of US 2005/0060562 (Bhattacharya et al.). In numbered paragraph 9, bridging pages 7 and 8 of the Office Action, claim 10 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over US 2003/0176940 (Rangachari et al.), in view of the Nazzal publication, and in further view of Symantec Antivirus for Macintosh copyright 1994. These rejections are respectfully traversed.

Applicant has disclosed quantitative data carrying meaningful information about the state of an IT part of a process control system and potential security events (e.g., page 8, lines 1 and 2). Such quantitative data can be obtained from routers, switches, proxies, host and application logs and performance counters, as well as a statistical IDS (e.g., page 8, lines 3 and 4).

Processing modules are disclosed which can convert raw input data into quantitative information to be presented to a user. Such quantitative data can enable a human process operator to make decisions as to the severity of an overall situation on the network (e.g., page 8, lines 5-6; page 10, lines 14 and 15; Fig. 2). The quantitative information can be presented to the human process operator in a simple format, having consistent principles (e.g., page 8, lines 20-22). Such an exemplary network security system presents quantitative variables for the human process operator to detect and decide upon the anomalies in the network based on a view of the displayed quantitative variables.

The foregoing features are broadly encompassed in claim 1, which recites a network security system for detecting security relevant irregularities in a network, including among other recited features, at least one processing module, connected to an input module for access to data sources, with means for translating network-security relevant data into quantitative variables; a supervisory system, with means for presenting the quantitative variables to a security system operator; and an interface module, with means for transferring said quantitative variables from the processing module to the supervisory system.

Regarding claim 1, the Nazzal publication does not present a basic quantitative variable of network security data to a security system operator. Instead, an intrusion detection according to the Nazzal publication is processed by the automated system to produce and display an output representing whether there is a network security anomaly. The Nazzal publication is directed to automated minimization of false assertions of a network intrusion, with no apparent role for the user other than passively viewing the displayed result.

The Nazzal publication does not specifically disclose translating network-security relevant data into quantitative variables in order to present the quantitative variables to a security system operator. Accordingly, the Nazzal publication would not have taught or suggested a network security system for detecting security relevant irregularities in a network, including among other features, at least one processing module, connected to an input module for access to data sources, with means for translating network-security relevant data into quantitative variables; a supervisory system, with means for presenting the quantitative variables to a security system operator; and an interface module, with means for transferring said

quantitative variables from the processing module to the supervisory system, as recited in claim 1.

The Symantec publication and the Bhattacharya et al. publication do not cure the deficiencies of the Nazzal publication. Rather, the Symantec publication relates to suspicious activity alerts via an alert box as shown in Fig. 4-6, and was applied in combination by the Examiner to reject dependent claim 4. The Bhattacharya et al. publication shows a hotspot vector graph in Figure 4, having level-structures as shown in Figure 5, and was applied in combination by the Examiner to reject dependent claim 7. However, even if the Nazzal publication, the Symantec publication and the Bhattacharya et al. publication were to have been considered in various combinations as the Examiner has suggested, the references would not have taught or suggested a network security system for detecting security relevant irregularities in a network, including among other recited features, at least one processing module, connected to an input module for access to data sources, with means for translating network-security relevant data into quantitative variables; a supervisory system, with means for presenting the quantitative variables to a security system operator; and an interface module, with means for transferring said quantitative variables from the processing module to the supervisory system, as recited in claim 1.

Regarding claim 10, claim 10 depends from claim 1. The Rangachari et al. publication describes an automation system for a semiconductor fabrication plant. As relied upon by the Examiner, the Rangachari et al. publication would not have taught or suggested the above network security system features for detecting security relevant irregularities as recited for claim 1. In further support of these

claimed features, claim 10 recites, among other features, a supervisory system integrated into an automation system controlling means, the quantitative variables being included in the information displaying system of the human machine interface, and a countermeasures initiating means being integrated in a commands entering means. Figs. 4 and 5 of the Rangachari et al. publication, in combination with the Nazzal publication and the Symantec publication as the Examiner has suggested, would not have taught or suggested these features recited in claim 10.

In view of the foregoing, claims 1, 4, 7 and 10 are patentable. The remaining claims depend from the independent claim and recite further advantageous features which further distinguish over the documents relied upon by the Examiner. Withdrawal of the rejections is respectfully requested.

Conclusion

From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested and such action is earnestly solicited.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: February 2, 2009 By: _____

Richard J. Kim, Reg. No. 48360
/for/ Patrick C. Keane, Reg. No. 32858

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620